UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re Morgan Stanley Data Security Litigation	20-cv-5914 (AT)

ORAL ARGUMENT REQUESTED

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT MORGAN STANLEY SMITH BARNEY LLC'S MOTION TO DISMISS

Paul, Weiss, Rifkind, Wharton & Garrison LLP
1285 Avenue of the Americas
New York, NY 10019
(212) 373-3000

2001 K Street NW
Washington, DC 20006
(202) 223-7300

Attorneys for Defendant

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Defendant Morgan Stanley Smith Barney LLC ("Morgan Stanley" or "the Company") respectfully submits this memorandum of law in support of its motion to dismiss the Consolidated Amended Complaint ("Complaint" or "CAC") (ECF No. 39) pursuant to Fed. R. Civ. P. 12(b)(1) or 12(b)(6).

PRELIMINARY STATEMENT

Unlike the typical data breach lawsuit, this case does ***not*** involve the exposure of any personal or financial information, any malicious actors, a deliberate cyberattack, phishing or malware. Rather, this case arises out of two incidents that occurred in 2016 and 2019, respectively. The first involved computer equipment that Morgan Stanley's vendors were supposed to wipe clean and/or destroy; however, Morgan Stanley later discovered that certain devices still contained some unencrypted data. The second relates to branch office computer equipment that was disconnected and replaced; after an inventory, Morgan Stanley was unable to locate a small number of those devices. Following an in-depth investigation in consultation with internal and outside technical experts and continual monitoring for potential misuse of any data derived from any Morgan Stanley source, Morgan Stanley has not become aware of a single instance of its customers' personally identifiable information ("PII") being accessed or misused in connection with either event. On July 10, 2020, Morgan Stanley provided information regarding these two data security events to potentially impacted customers and to the State Attorneys General. (*See* O'Brien Decl. Ex. 1, Consumer Notice of Data Breach (ECF 1-1) (hereinafter, "Consumer Notice") and O'Brien Decl. Ex. 2, Notice of Data Breach to State Attorney General (ECF 1-2) (hereinafter "Attorneys General Notice").)[1]

[1] Citations to "O'Brien Decl." refer to the Declaration of Jane O'Brien in Support of the Memorandum of Law in Support of Defendant's Motion to Dismiss, filed herewith. The Court may consider the Consumer Notice and the Attorneys General Notice because the

On the heels of that notice, eight separate lawsuits were filed and later consolidated into the single proceeding now before this Court. In their Complaint, named plaintiffs John and Midori Nelson, Sylvia Tillman, Mark Blythe, Vivian Yates, Richard and Cheryl Gamen, Amresh Jaijee, Richard Mausner, Desiree Shapouri, and Howard Katz—individuals residing in California, Florida, Illinois, New York, New Jersey, and Pennsylvania—purport to advance myriad common law and statutory claims arising out of these events on behalf of a putative class. However, their Complaint suffers from several fundamental and dispositive flaws.

First, the Complaint is (unsurprisingly) devoid of plausible allegations that any of plaintiffs' or the proposed class members' personal data was ever accessed or misused as a result of the data events, or any other cognizable injury. Thus, plaintiffs lack Article III standing to pursue any of their claims. None of the plaintiffs have alleged suffering any purported injury prior to June 2019, rendering any claims arising out of the 2016 incident purely speculative. Nor do any of the four theories advanced by plaintiffs establish a credible injury-in-fact with respect to either incident: (i) plaintiffs' allegations that they face injury due to the possibility of their data being misused are too attenuated to establish standing; (ii) plaintiffs fail plausibly to allege that the events diminished the value of their PII; (iii) their claim of standing based on so-called "out-of-pocket expenses" associated with the prevention of misuse of PII is deficient as a matter of law; and (iv) plaintiffs' allegations that they suffered injuries in the form of annual fees or other similar payments to Morgan Stanley are too vague and conclusory to confer standing.

Complaint relies heavily on their terms and effect and they are therefore integral to the Complaint. *See Chambers* v. *Time Warner, Inc.*, 282 F.3d 147, 152–53 (2d Cir. 2002); *see also* CAC ¶¶ 5, 16-24, 37-39. The Consumer Notice and the Attorneys General Notice were also attached to the original complaint filed in this action and incorporated by reference therein. *See* ECF 1-1 and 1-2.

Second, the Complaint should be dismissed with prejudice for the independent reason that plaintiffs fail to state a claim under Fed. R. Civ. P. 12(b)(6). Each cause of action asserted is deficient: (i) plaintiffs' negligence claim fails because they have not alleged that Morgan Stanley breached any general or specific duty of care, or that plaintiffs suffered any damages; (ii) New York law does not recognize a claim for invasion of privacy in the data breach context or a "breach of confidence" claim as pleaded by plaintiffs in the context of a data breach action; these claims also should be dismissed because plaintiffs have failed to adequately plead damages; (iii) the unjust enrichment claim is duplicative of plaintiffs' common law tort claims and fails to plausibly plead that Morgan Stanley was enriched at plaintiffs' expense; and (iv) the plaintiffs fail to plead the elements of the state statutory claims.

For these reasons and as set forth more fully below, the Complaint should be dismissed in its entirety and with prejudice.

STATEMENT OF FACTS

In 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment associated with those centers. (CAC ¶ 6.) The Company hired a vendor to remove data on hardware stored in the two data centers. (*Id*.) Morgan Stanley later learned that the vendor did not fully remove data from the decommissioned equipment, as it had been contractually required to do. (*Id*.) Morgan Stanley immediately took steps to investigate and recover the devices, and found no evidence that any customers' personal information was accessed or misused (the "2016 Event"). (*See* Ex. 1, Consumer Notice).

Separately, in 2019, Morgan Stanley disconnected and replaced multiple computer servers in local branch offices. (CAC ¶ 7.) Those servers had stored information on encrypted disks that may have included personal information. (*Id*.) In a subsequent inventory,

the Company determined that it was unable to locate a small number of those devices, and the manufacturer later informed Morgan Stanley of a software flaw that could have resulted in small amounts of previously deleted information remaining on the disks in unencrypted form (the "2019 Event"). (*Id.*; *see also* Ex. 2 at 3, Attorneys General Notice.)

Upon learning of each of these events, Morgan Stanley undertook thorough investigations and worked with internal and outside technical experts to understand whether there was any potential risk to customer data. Morgan Stanley has also continuously monitored internet and "dark web" forums for any evidence of misuse of Morgan Stanley customer data and has not detected any unauthorized activity related to these incidents. (Ex. 2 at 1, Attorneys General Notice.) On July 10, 2020, Morgan Stanley sent a notice of security incident to provide information to individuals whose data may have been on the devices; in the notices, Morgan Stanley affirmed that it was "not aware of any access to, or misuse of, . . . personal information in connection with either incident" and offered fraud monitoring and identity theft-related services at no cost to customers. (*Id.* at 1–2.)

Each of the named plaintiffs alleges that he or she received Morgan Stanley's July 2020 notice (CAC ¶¶ 16-24), but provides scant further detail of their accounts with Morgan Stanley or how each plaintiff purports to have been injured by the data events. Plaintiffs principally assert conclusory and boilerplate allegations of harm, including that (i) they have been injured because they face impending data theft sometime in the future, notwithstanding that there is no allegation that their data was in fact accessed by or exposed to third parties as a result of either event (*see id.* ¶¶ 103, 114, 125, 135, 147, 159, 168, 178, and 188); (ii) the value of their PII has diminished, although there is no allegation as to what value their PII had to plaintiffs to begin with, how either of the security events impacted the value of their PII in any way, or any

efforts by plaintiffs to monetize their PII (*id.* ¶¶ 101, 112, 123, 133, 145, 157, 166, 176, 186); (iii) they have experienced lost time, annoyance, interference, and inconvenience as a result the alleged data breach incidents (*id.* ¶¶ 102, 113, 124, 134, 146, 158, 167, 177, 187); and they have made unspecified payments to Morgan Stanley (*id.* ¶¶ 100, 111, 122, 132, 144, 156, 165, 175, 185).

For just five of the eleven named plaintiffs, the Complaint includes the following additional, albeit still insufficient, allegations:

- Desiree Shapouri alleges that in September 2019, she experienced twelve unauthorized charges on her American Express credit card. (CAC ¶ 172.) She does not allege that she ever provided information regarding her American Express account to Morgan Stanley—which is not the card issuer—or that her American Express account information was implicated in the 2016 or 2019 Events.

- Midori Nelson alleges that in June 2019, fraudulent purchases appeared on her credit card, and that the same thing occurred later in 2019. (*Id.* ¶ 97.) In both instances, the credit card confirmed the fraud, reimbursed the account, and replaced the card. (*Id.*) Ms. Nelson similarly does not allege that her credit card information had been provided to Morgan Stanley, or that it was implicated in either the 2016 or 2019 Events.

- Mark Blythe alleges that in July 2020, unauthorized third parties opened a checking account with a credit union in Mr. Blythe's name, applied for a Small Business Administration loan in his name, and opened a savings account in Mr. Blythe's name. (*Id.* ¶ 118.) There are no allegations tying these events to the 2016 or 2019 Events.

- Richard Gamen alleges that in June 2020, he began receiving scam telephone calls, which claim his Social Security number is "locked" and that he may be arrested. He has also alleged that he started receiving emails from fraudsters claiming a foreign person has died and the fraudster is reaching out to share the money. (*Id.* ¶ 140.) There are no allegations tying these events to the 2016 or 2019 Events.

- Amresh Jaijee alleges that in June 2020, she received a telephone call from an individual claiming to represent an insurance company, and that this individual knew her Social Security number and attempted to have her verify it and her bank routing number. (*Id.* ¶ 151.) She also alleges that since June 2020 she has received an increased number of scam telephone calls. (*Id.* ¶ 152.) Again, there are no allegations tying these events to the 2016 or 2019 Events.

None of the named plaintiffs purport to have suffered any injury prior to June 2019.

ARGUMENT

I. PLAINTIFFS CANNOT ESTABLISH ARTICLE III STANDING

Plaintiffs' Complaint should be dismissed for failure to allege facts sufficient to confer Article III standing for any of their claims, thus depriving this Court of subject matter jurisdiction. *See Carter* v. *HealthPort Techs., LLC*, 822 F.3d 47, 56 (2d Cir. 2016). Standing consists of three elements: (i) "the plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest"; (ii) "there must be a causal connection between the injury and the conduct complained of"; and (iii) "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan* v. *Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (citations and internal quotation marks omitted). Plaintiffs do not adequately allege that they "suffered an injury in fact that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." *Pena* v. *British Airways, PLC (UK)*, 18-cv-6278 (LDH) (RML), 2020 WL 3989055, at *2 (E.D.N.Y. Mar. 30, 2020) (*quoting Carver* v. *City of New York*, 621 F.3d 221, 225 (2d Cir. 2010)). Nor have they adequately alleged that any purported injury suffered can be attributed to Morgan Stanley. *See Garelick* v. *Sullivan*, 987 F.2d 913, 919 (2d Cir. 1993). Having failed to satisfy either the first or second prongs, plaintiffs cannot satisfy the redressability prong.[2]

Here, plaintiffs purport to plead injury-in-fact under four theories: (i) they allege that they face impending injury due to the likelihood of their data being misused (CAC ¶¶ 103, 114, 125, 135, 147, 159, 168, 178, 188); (ii) they allege that they have suffered injury in the form

[2] Additionally, in a putative class action such as this one, the "named plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong." *Ortiz* v. *CIOX Health LLC*, 386 F. Supp. 3d 308, 312 (S.D.N.Y. 2019) (*quoting Spokeo, Inc*. v. *Robins*, 136 S. Ct. 1540, 1547 n.6 (2016)).

of damages and diminution in the value of their PII (*id.* ¶¶ 101, 112, 123, 133, 145, 157, 166, 176, 186); (iii) they allege that they have experienced lost time, annoyance, interference, and inconvenience as a result the data breach incidents (*id.* ¶¶ 102, 113, 124, 134, 146, 158, 167, 177, 187); and (iv) they each allege that they paid "annual fees" or "money" to Morgan Stanley for facilitating their accounts which they allegedly would not have paid if Morgan Stanley had "disclosed that it lacked data security practices adequate to safeguard customers' PII" (*id.* ¶¶ 100, 111, 122, 132, 144, 156, 165, 175, 185). None of these allegations suffice to establish standing.

First, plaintiffs' allegations that they have been injured as a result of the mere likelihood of their data being misused in the future are too attenuated to establish standing. This is particularly true here, where plaintiffs have only made conclusory allegations that any of the data involved in the two data incidents has or is likely to be misused and have made no allegations of theft of or access to plaintiffs' PII by malicious actors. While allegations of future harm "may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur," *Susan B. Anthony List* v. *Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)), "[a]llegations of *possible* future injury are not sufficient." *Clapper*, 568 U.S. at 409 (emphasis in original). Indeed, to establish standing, a future injury must be "certainly impending," and a "theory of standing [] which relies on a highly attenuated chain of possibilities[] does not satisfy the requirement that threatened injury must be certainly impending." *Id*. at 410.

There is a growing consensus that in order to demonstrate standing for a data breach claim, plaintiffs must allege that data has been stolen by third parties, hackers, or cyber criminals who had intentionally targeted the data. *See Steven* v. *Carlos Lopez & Assocs., LLC*,

422 F. Supp. 3d 801, 804 (S.D.N.Y. 2019) (allegations that a plaintiff's data has been "targeted and taken by one or more unauthorized parties" for malicious purposes, rather than simply exposed to unauthorized parties, are the "common denominator" separating the data security cases in which circuit courts have found standing from those in which courts have rejected standing) (citation and internal quotation marks omitted). That is **not** what happened here, and plaintiffs do not—indeed cannot—allege otherwise. Allegations of misuse—or, at the very least, theft—are crucial for standing purposes because the "intentional act of theft [gives] rise, in turn, to a plausible inference that the stolen data [will] be misused." *Id.* at 805. Absent such allegations of intentional theft or data misuse, plaintiffs, like the plaintiffs in this case, can show only an "attenuated chain" of inferences "that at some unspecified point in the indefinite future they will be the victims of identity theft," which is insufficient to confer standing. *Id.* at 806 (internal citations and quotation marks omitted).

Circuits that have considered this question have also agreed that, to establish standing, plaintiffs must allege that data was stolen with the intent to improperly access or misuse PII. *See Katz* v. *Pershing, LLC*, 672 F.3d 64, 79 (1st Cir. 2012) (standing is not established where plaintiff "has not alleged that [its] nonpublic personal information actually has been accessed by any unauthorized person,"); *Reilly* v. *Ceridian Corp.*, 664 F.3d 38, 40–44 (3d Cir. 2011) (where there "has been no misuse of the information, [there is] no harm"); *Beck* v. *McDonald*, 848 F.3d 262, 274–76 (4th Cir. 2017) (the "mere theft" of a device containing PII, "without more, cannot confer Article III standing").[3]

[3] Other Circuits have held that a risk of injury is a risk sufficient to establish standing, but each of those cases involved an intentional hack. For example, *In re U.S. Office of Personnel Management Data Security Breach Litigation* involved an intentional hack and the sensitive data was in the hands of malicious actors (*i.e.*, hackers). 928 F.3d 42, 55–57 (D.C. Cir. 2019). The court noted, in citing previous precedent, that "it was reasonable to infer that the

Though the Second Circuit has not yet squarely addressed the issue of standing for a plaintiff alleging injury based on the possibility of future harm in a data breach case, in an unpublished decision, the Court emphasized that a plaintiff must show that identity theft or misuse of the data is "'certainly impending,' rather than simply speculative" or a mere possibility. *See Whalen* v. *Michaels Stores, Inc.*, 689 F. App'x 89 (Mem.), 90–91 (2d Cir. 2017) (summary order) (quoting *Clapper*, 568 U.S. at 409).[4]

---

cyberattackers had 'both the intent and the ability to use that data for ill.'" *Id.* at 56. *Galaria* v. *Nationwide Mutual Insurance Co.* likewise involved an intentional hack, and the court emphasized the importance of the fact that "Plaintiffs allege an 'identifiable taking'—the intentional theft of their data.'" 663 F. App'x 384, 389–90 (6th Cir. 2016). *Dieffenbach* v. *Barnes & Noble, Inc*. also involved an intentional hack of payment PIN pads. 887 F.3d 826, 827–30 (7th Cir. 2018). While the court found that costs of mitigation were concrete losses, they all stemmed from mitigations against a risk that actually came to fruition, i.e. hackers taking money from plaintiffs' bank accounts. *Id.* at 829. *In re Zappos.com, Inc. Customer Data Security Breach Litigation* too, involved an intentional hack, 888 F. 3d 1020, 1025–27 (9th Cir. 2018); the court there referred to *Krottner* v. *Starbucks Corp*., the operative Ninth Circuit precedent, which observed that had no data device been stolen and had plaintiffs merely "sued based on the risk that [the data device] would be stolen at some point in the future," then the threat of harm would be "far less credible." 628 F.3d 1139, 1143 (9th Cir. 2010).

[4] District courts across the country have reached similar conclusions and dismissed data breach complaints for lack of standing where the data was not alleged to have been obtained or used by bad actors. *See, e.g.*, *Randolph* v. *ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007); *U.S. Hotel & Resort Mgmt., Inc.* v. *Onity, Inc.*, Civil No. 13-1499 (SRN/FLN), 2014 WL 3748639, at *5 (D. Minn. July 30, 2014) ("In the 'lost data' context, where the courts have split somewhat on the question of standing, it now appears that a majority of the courts to have addressed the 'lost data' issue hold that plaintiffs whose confidential data has been exposed, or possibly exposed, by theft or a breach of an inadequate computer security system, but who have not yet had their identity stolen or their data otherwise actually abused, lack standing to sue the party who failed to protect their data." (citing *Reilly*, 664 F.3d at 43)); *Blahous* v. *Sarrell Reg'l Dental Ctr. for Pub. Health, Inc.*, 2:19-cv-798-RAH-SMD, 2020 WL 4016246, at *5–7 (M.D. Ala. July 16, 2020) (noting "lower federal courts presented with 'lost data' or potential identity theft cases in which there is no proof of *actual* misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data"); *Engl* v. *Natural Grocers by Vitamin Cottage, Inc.*, 15-cv-02129-MSK-NYW, 2016 WL 8578252, at *5 (D. Colo. Sept. 21, 2016) ("[T]he risk of future injury alone is not sufficient [in] cases where a data breach merely exposes data to those who might use it, but in cases where there is indicia that hackers have actually obtained and used the data, there is a present [*sic*] a risk of future injury sufficient to support standing.")

Here, plaintiffs plainly concede that "[t]his case does not involve a breach of a computer system by a third party," and rather speculate (without plausible supporting facts) that Plaintiffs' PII was "disclos[ed] . . . to unknown third parties." (CAC ¶ 4.) The Complaint therefore does not plausibly allege any misuse of or improper access to their information. Plaintiffs provide boilerplate assertions that they face "the substantially increased risk of fraud, identity theft, and misuse" (*id.* ¶¶ 103, 114, 125, 135, 147, 159, 168, 178, 188), but those allegations fall far short of pleading a plausible claim that "certainly impending" risk that actual harm will occur. *See Cherny* v. *Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) ("The Court finds that [the plaintiff's] concern that his confidential information may at some point be acquired is 'solely the result of a perceived and speculative risk of future injury that may never occur.'" (quoting *Shafran* v. *Harley-Davidson, Inc.*, No. 07 Civ. 01365, 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008)).

Elsewhere, five of the eleven named plaintiffs allege scattered instances of recent attempts at credit card theft, phishing, or spamming—all occurring *after* June 2019. As an initial matter, it strains credulity to claim that these events were caused by the 2016 Event, given the passage of time. At a minimum, claims arising out of the 2016 Event should be dismissed from

---

(emphases in original); *Whitaker* v. *Health Net of Cal., Inc.*, No. CIV S-11-0910 KJM-DAD, 2012 WL 174961, at *3 (E.D. Cal. Jan. 20, 2012) (holding plaintiffs lacked standing because they alleged that their data was lost and not stolen and "do not explain how the loss here has actually harmed or threatens to harm them, or that third parties have accessed their data."); *Kimbriel* v. *ABB, Inc.*, 5:19-CV-215-BO, 2019 WL 4861168, at *2–3 (E.D.N.C. Oct. 1, 2019) (holding plaintiffs failed to establish Article III standing for claims arising from data breach where the only alleged harm was scattered instances of credit inquiries); *Stapleton on behalf of C.P.* v. *Tampa Bay Surgery Ctr., Inc.*, 8:17-cv-1540-T-30AEP, 2017 WL 3732102, at *3 (M.D. Fla. Aug. 30, 2017); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25–26 (D.D.C. 2014); *Crisafulli* v. *Amertias Life Ins. Corp.*, No. 13-5937, 2015 WL 1969176, at *4 (D.N.J. Apr. 30, 2015); *Storm* v. *Paytime, Inc.*, 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015).

this case. Plaintiffs cannot plausibly link them to Morgan Stanley, and, unsurprisingly, have made no more than conclusory allegations to overcome that disability. (CAC ¶¶ 97, 118, 140, 151–152, 172.) Two of these five plaintiffs—Desiree Shapouri and Midori Nelson—allege that their credit card information was misused, but the Complaint concedes that credit card numbers were not exposed in either of the alleged data breach incidents. (*Id*. ¶¶ 40, 53.) The other three plaintiffs—Richard Gamen, Amresh Jaijee, and Mark Blythe—allege that they experienced various instances of spamming and potential identity fraud in either June or July 2020. While that timing coincides with plaintiffs' receipt of the Consumer Notice, it is not sufficiently close in time to either the 2016 or 2019 Events to plausibly allege causation. (*See* CAC ¶¶ 118, 140, 152.) Accordingly, plaintiffs cannot show traceability between the purported harm they have suffered and Morgan Stanley's conduct. *See, e.g.*, *Welborn* v. *IRS*, 218 F. Supp. 3d 64, 79–80 (D.D.C. 2016) (holding traceability element of standing not satisfied where plaintiff "simply allege[d] that the alleged financial fraud happened *after*" the breach without showing that "the type of data obtained from the theft" was misused). Indeed, courts are "usual[ly] reluctan[t] to endorse standing theories that rest on speculation about the decisions of independent actors," *Clapper*, 568 U.S. at 414, especially where the theory rests on "speculation" or conjecture about a future unlawful injury. *Los Angeles* v. *Lyons*, 461 U.S. 95, 105 (1983) (past exposure to illegal conduct was insufficient to establish a risk of future unlawful injury). *See also*, *Elec. Privacy Info. Ctr.* v. *U.S. Dep't of Commerce*, 928 F.3d 95, 102 (D.C. Cir. 2019), *cert. denied sub nom. Elec. Privacy Info. Ctr.* v. *Dep't of Commerce*, 140 S. Ct. 2718 (2020). Because plaintiffs' standing theory depends on the intervening, illegal acts of third-party actors, plaintiffs have failed to properly plead, beyond a "speculative level" that they face injury due to the likelihood of their data being misused. *Bell Atl. Corp.* v. *Twombly,* 550 U.S. 544, 555 (2007).

Second, plaintiffs fail to allege that the data events diminished the value of their PII, because they have not alleged any particular value of which they have been deprived. *See, e.g.*, *Pena* v., 2020 WL 3989055, at *3 ("[A]ssuming Plaintiff's personal information has value, Plaintiff has failed to allege any facts indicating how Defendant's data breach diminished that value in any way."). Rather, they repeatedly allege in a simplistic and conclusory fashion that each plaintiff "suffered actual injury in the form of damages to and diminution in the value of [his or her] PII—a form of intangible property." (*See* CAC ¶¶ 101, 112, 123, 133, 145, 157, 166, 176, 186.)

Third, plaintiffs also purport to allege standing based on so-called "out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their PII" and "lost opportunity costs associated with attempting to mitigate the actual consequences of" the 2016 and 2019 Events, "including but not limited to lost time." (CAC ¶ 14.) But plaintiffs' own allegations reflect that Morgan Stanley rendered these expenditures unnecessary by maintaining "continuous fraud monitoring and monitoring of information about malicious online activity and evidence of misuse of any Morgan Stanley data" (*id.* ¶ 42), and offering potentially affected clients automatic and complimentary "two years of credit monitoring service." (*Id.* ¶ 61.) In any event, courts routinely reject attempts by plaintiffs to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Steven*, 422 F. Supp. 3d at 807 (holding plaintiffs cannot justify standing based on their "time and money spent monitoring or changing their financial information and accounts" after a data breach, and collecting cases

(internal quotation marks omitted and quoting *Clapper*, 133 S. Ct. at 1151)).[5] While mitigation efforts may establish standing in cases where the underlying breach is tied to actions of a bad actor, that is not the case here. *Cf. id.*, 422 F. Supp. 3d at 805-06; *see also Rudolph* v. *Hudson's Bay Co.*, 18-cv-8472 (PKC), 2019 WL 2023713, at *1 (S.D.N.Y. May 7, 2019) (mitigation efforts conferred standing where payment-card database was breached by a group of hackers); *Fero* v. *Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 335 (W.D.N.Y. 2018) (mitigation efforts conferred standing where computer network systems was hacked by a third-party); *In re Capital One Consumer Data Sec. Breach Litig.*, 1:19-md-2915 (AJT/JFA), 2020 WL 5629790, at *2 (E.D. Va. Sep. 18, 2020) (mitigation efforts conferred standing where "unauthorized individual" hacked into internal servers); *In re Marriott Int'l Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 454 (D. Md. 2020) (mitigation efforts conferred standing where hackers breached the guest information database).

Fourth, plaintiffs offer conclusory allegations that they suffered injury through payments of fees or money to Morgan Stanley for "facilitating" their accounts and that they would not have made these payments "had [Morgan Stanley] disclosed that it lacked data security practices adequate to safeguard customers' PII." (*See* CAC ¶¶ 100, 111, 122, 132, 144, 156, 165, 175, 185.) But nowhere do plaintiffs plead what these payments were for, or that they were at all connected to storage of plaintiffs' PII (as opposed to the numerous financial services Morgan Stanley provided that were the core purposes of plaintiffs' various accounts), that data

[5] *See also In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) ("Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury."); *Beck*, 848 F.3d at 276–77 ("[S]elf-imposed harms cannot confer standing."); *Cherny*, 604 F. Supp. 2d at 609 ("Courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury the law is prepared to remedy." (quotation and citation omitted)).

security practices at Morgan Stanley impacted plaintiffs' decision to use Morgan Stanley over another financial institution, or otherwise connecting the payments to either data event. These threadbare allegations of payments made to Morgan Stanley are too attenuated to confer standing. *Lujan*, 504 U.S. at 564 n.2; *see also Jackson* v. *Loews Hotels, Inc.*, No. ED CV 18-827-DMG, 2019 WL 6721637, at *2 (C.D. Cal. July 24, 2019) ("Plaintiffs have identified no authority approving of a 'benefit of the bargain' theory in a data breach case based on such conclusory allegations of an *implied* promise to earmark a portion of the purchase price for ensuring data safety. Indeed, case law appears to require more precise allegations and more explicit promises." (emphasis in original) (citing *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015)). For all of these reasons, plaintiffs fail to establish standing and their Complaint should be dismissed.

II. PLAINTIFFS FAIL TO ADEQUATELY PLEAD ANY OF THEIR CLAIMS

Even if plaintiffs had established Article III standing, which they have not, the Complaint should be dismissed with prejudice for failure to state a claim under Fed. R. Civ. P. 12(b)(6). Although the material facts alleged in the complaint are to be treated as true at the pleading stage, "a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly,* 550 U.S. at 555 (citation and internal quotation marks omitted). To survive a motion to dismiss, a complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Id*. As discussed below, plaintiffs fail to meet this standard with respect to each of their claims.

A. Plaintiffs Fail to State a Claim for Negligence

"Under New York law, in order to recover on a claim for negligence, a plaintiff must show (1) the existence of a duty on defendant's part as to plaintiff; (2) a breach of this duty;

and (3) injury to the plaintiff as a result thereof." *Caronia* v. *Philip Morris USA, Inc.*, 715 F.3d 417, 428 (2d Cir. 2013) (citation and internal quotation marks omitted). Plaintiffs' negligence claim fails because they have not alleged that Morgan Stanley breached any general or specific duty of care, nor any injury.

Beyond entirely boilerplate, conclusory allegations, plaintiffs fail to plausibly allege how Morgan Stanley's data security practices deviated from acceptable industry custom or practices to plead either the existence of a duty or a breach thereof. (*See* CAC ¶¶ 226–259.) For example, plaintiffs assert that Morgan Stanley "had a duty to exercise reasonable care in safeguarding, securing, and protecting . . . information" (without alleging what the source of that duty was) (*id.* ¶ 231); that it "had a duty to exercise appropriate clearinghouse practices" (without identifying what those clearinghouse practices were or should have been) (*id.* ¶ 232); and that it "had a duty to have procedures in place to detect and prevent the improper access and misuse" of PII (without alleging that Morgan Stanley failed to protect the misuse of plaintiffs' PII) (*id.* ¶ 233).[6] These conclusory and formulaic pleadings fail plausibly to allege that specific data security practices at Morgan Stanley were deficient or deviated from an acceptable industry baseline or standard to state a claim for negligence. *See, e.g.*, *MLSMK Inv. Co.* v. *JP Morgan Chase & Co.*, 431 F. App'x 17, 20 (2d Cir. 2011) (summary order) (affirming dismissal of

[6] While plaintiffs purport to allege that they were in a "special relationship" Morgan Stanley, they do not identify the source of that special relationship beyond an ambiguous, "'independent duty,' untethered to any contract between" Morgan Stanley and any named plaintiff. (CAC ¶¶ 234-235.) Such allegations are insufficient to establish any cognizable duty. A "special relationship" can only give rise to a duty to protect an individual from the conduct of others in limited circumstances, none of which are present here. *See Fay* v. *Assignment Am.*, 666 N.Y.S.2d 304, 306 (3d Dep't 1997) ("Examples of . . . special relationships include the relationship between employers and employees, parents and children, common carriers and their patrons, and school districts and their students, among others.").

negligence claim because the allegations of breach of duty were conclusory and insufficient to state a claim).

Even if these allegations demonstrated a breach of a duty (they do not), plaintiffs do not adequately plead the elements of causation or damages. First, as mentioned *supra* at Part I, plaintiffs have not alleged any cognizable harm or injury. *See, e.g.*, *Willey* v. *J.P. Morgan Chase, N.A.*, No. 09 Civ. 1397 (CM), 2009 WL 1938987, at *9 (S.D.N.Y. July 7, 2009) ("Because [plaintiff] does not allege that any of his personal data (or anyone else's for that matter) was actually misused, he has not alleged damages sufficient to support his state law claims [including negligence]."); *Caudle* v. *Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 276 (S.D.N.Y. 2008) (dismissing at summary judgment a negligence claim where plaintiff had not alleged that anyone had attempted to access or use the laptop containing PII, and observing that, in a case alleging potential misuse of PII, damages must be "reasonably certain to be incurred" to be recoverable). Even if plaintiffs could show that they were harmed, they have alleged no facts plausibly linking that purported harm to anything Morgan Stanley did (or failed to do). *See, e.g.*, *Mortensen* v. *Mem'l Hosp*., 483 N.Y.S.2d 264, 270 (1st Dep't 1984) (to demonstrate causation, a defendant's negligent act must have been a "substantial factor in bringing about the plaintiff's injury."). Causation is all-the-more implausible here, considering that more than five years has passed since the 2016 Event and the alleged injury depends on the superseding criminal acts of third parties. *Cf. Deskovic* v. *City of Peekskill*, 673 F. Supp. 2d 154, 161 (S.D.N.Y. 2009) ("Generally, an intervening intentional or criminal act is a type of superseding cause that severs the liability of the original tort-feasor.").

As for plaintiffs' negligence *per se* claim, under New York state law, Section 5 of the FTC Act cannot support a claim for negligence. *See Smahaj* v. *Retrieval-Masters Creditors*

Bureau, Inc., 69 Misc. 3d 597, 608 (N.Y. Sup. Ct. Westchester Cty. 2020) (in a putative class action founded on an alleged data breach, the court held that "Plaintiff's negligence *per se* claim based on an alleged violation of the FTC Act must also be dismissed" because a negligence *per se* claim is one that the statute "does not recognize") (*quoting Lugo* v. *St. Nicholas Assoc.*, 2 Misc. 3d 212, 218 (N.Y. Sup. Ct. NY Cty. 2003), *aff'd* 18 A.D.3d 341, 795 (1st Dep't 2005); *cf. In re SuperValu, Inc.*, 925 F.3d 955, 963–64 (8th Cir. 2019) (applying Illinois law). For these reasons, plaintiffs fail to state a claim for negligence or negligence *per se*.

B. Plaintiffs Fail to State a Claim for Invasion of Privacy or Breach of Confidence

Plaintiffs fail to state a claim for invasion of privacy or breach of confidence both because (i) New York does not recognize either cause of action and (ii) they have failed adequately to plead the element of damages.

First, New York law, which plaintiffs agree governs their common law claims (CAC ¶ 224), has abolished the common law tort of invasion of privacy. *See Nerhanu* v. *N.Y. State Ins. Fund*, No. 91 CIV. 4956 BSJ, 1999 WL 813437, at *19 (S.D.N.Y. Oct. 8, 1999) ("New York does not recognize a common law cause of action for invasion of privacy . . . Instead, New York recognizes only a limited privacy cause of action, pursuant to statute, for appropriation of one's name or likeness for commercial purposes." (internal citation omitted)). Specifically, sections 50 and 51 of the New York Civil Rights Act provide the exclusive remedy for invasion of privacy, and only apply in limited circumstances, such as the use of a person's physical likeness.[7]

[7] *See, e.g.*, *Cohen* v. *Herbal Concepts*, 63 N.Y.2d 379, 383–84 (1984) (providing a comprehensive discussion of the history of New York privacy law and noting the "statute is designed to protect a person's identity, not merely a property interest in his or her name 'name,' 'portrait' or 'picture,' and thus it implicitly requires that plaintiff be capable of identification from the objectionable material itself"); *Brighton* v. *McIntosh*, No. 10 Civ.

While plaintiffs have argued that their claim falls under Civil Rights Law §§ 50 and 51 because those statutes preclude the "use[] . . . for the purposes of trade, the name . . . of any living person without having first obtained the written consent of such person" (*see* ECF No. 45 at 3), that theory fails because plaintiffs make no allegation that Morgan Stanley actually used their names for purposes of trade. Although the Complaint makes a passing reference to Morgan Stanley's AI Center of Excellence (*see* CAC ¶¶ 84–85), there is no allegation whatsoever that Morgan Stanley uses customer names in the Center of Excellence, how such use—if it ever occurred—was for purposes of trade, or how the AI Center of Excellence has any connection to the devices at issue.

Second, New York courts have not recognized a nebulous "breach of confidence" claim of the sort asserted by plaintiffs—i.e., arising independently from either a fiduciary or contractual relationship (*see* CAC ¶ 235)—in the context of a data breach action. *In re Capital One Consumer Data Sec. Breach Litig.*, 1:19-md-2915, 2020 WL 5629790, at *18 n.21 (E.D. Va. Sept. 18, 2020) ("The Court is not aware of any decision under [New York] law that has recognized a tort for the breach of confidence within the context of a bank/customer relationship. And in fact, New York courts have expressed reluctance to recognize such a tort." (citing *Young* v. *U.S. Dep't of Justice*, 882 F.2d 633, 637 (2d Cir. 1989)); *Graney Dev. Corp.* v. *Taksen*, 92 Misc. 2d 764 (N.Y. Sup. 1978), *aff'd*, 66 A.D.2d 1008 (4th Dep't 1978)). *See also, Young*, 882 F.2d at 640–41 (noting "[a]t this point, New York courts have recognized [a breach-of-confidence theory] only in the context of physician-patient relationships" and that "New York's

8282 (PKC), 2011 WL 3585982, at *3 (S.D.N.Y. July 28, 2011) (Section 50 and 51 are "narrowly construed"); *Farrow* v. *Allstate Ins. Co.*, 53 A.D.3d 563, 563–64 (2d Dep't 2008) (New York invasion of privacy claims are limited to protecting against "appropriation of a plaintiff's name or likeness for a defendant's benefit").

courts have been rather conservative in recognizing causes of action for damages in the privacy field" and ultimately holding that, due to the undeveloped nature of this area of New York state law, *Colorado River* abstention was warranted); *Madden* v. *Creative Servs., Inc.*, 84 N.Y.2d 738, 744–47 (1995) (noting New York courts only sometimes recognize breach of confidence claims in narrow circumstances "premised on [a] violation of a fiduciary or contractual relationship").[8]

Finally, in any event, both of these claims fail because, for all the same reasons plaintiffs lack standing, they have failed to allege any cognizable damages resulting from either incident. Indeed, even where a plaintiff can establish standing, allegations of damages to adequately plead a substantive claim may still fail. *See, e.g.*, *Attias* v. *CareFirst, Inc.*, 365 F. Supp. 3d 1, 9 (D.D.C. 2019) ("Plaintiffs may satisfy the Article III injury-in-fact requirement and yet fail to adequately plead damages for a particular cause of action."). Where, as here, plaintiffs' claim is merely that "they have a heightened fear of having their identities stolen in the future and have, as a result, taken steps to monitor their credit more vigilantly," these allegations lack a "high degree of probability that a future injury will occur" for purposes of pleading damages for negligence. *Hammond* v. *Bank of N.Y. Mellon Corp*., No. 08 Civ. 6060 (RMB)(RLE), 2010 WL 2643307 at *10 (S.D.N.Y. June 25, 2010); *see also Caudle*, 580 F. Supp. 2d at 282 ("New York would not allow a negligence [claim] to proceed" where no factors demonstrating a serious concern over misuse of stolen data were present).

---

[8] Plaintiffs have argued, based on *Daly* v. *Metropolitan Life Ins. Co*., 782 N.Y.S.2d 530, 535-36 (Sup. Ct. 2004), that a breach of confidence claim has been recognized by New York courts. (*See* ECF No. 45 at 3.) That argument fails, however, because *Daly* analyzed claims for negligence, not a standalone breach of confidence claim. *See also Jones* v. *Commerce Bank, N.A.,* No. 06CIV835HB, 2007 WL 672091, at *3 (S.D.N.Y. Mar. 6, 2007) (applying *Daly* to a claim for negligence). Furthermore, *Daly* involved confidential information transferred in the context of a fiduciary relationship, which the court found could generate a duty under the laws of negligence. Here, by contrast, plaintiffs have not alleged any fiduciary relationship between them and Morgan Stanley.

C. Plaintiffs Fail to State a Claim for Unjust Enrichment

To state a claim for unjust enrichment under New York law, a plaintiff must allege that "(1) defendant was enriched, (2) at plaintiff's expense, and (3) equity and good conscience militate against permitting defendant to retain what plaintiff is seeking to recover." *Briarpatch Ltd., L.P.* v. *Phoenix Pictures, Inc.*, 373 F.3d 296, 306 (2d Cir. 2004) (citing *Clark* v. *Daby*, 751 N.Y.S.2d 622, 623 (3d Dep't 2002)).

Plaintiffs' allegations fall far short of pleading a viable claim for unjust enrichment. (*See* CAC ¶¶ 272–285.) First, plaintiffs have failed to allege that Morgan Stanley engaged in any inequitable conduct accruing to its benefit. Second, plaintiffs' claim fails because they have not plausibly alleged that their PII has any value to Morgan Stanley. *See In re Jetblue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 330 (E.D.N.Y. 2005). Plaintiffs offer allegations about the value of PII to cybercriminals (CAC ¶¶ 49–55), but not to Morgan Stanley, which is necessary to satisfy the first element of an unjust enrichment claim. While plaintiffs allude to Morgan Stanley's AI Center of Excellence as a purported motive for collecting and retaining plaintiffs' PII (CAC ¶¶ 82–85), they do not allege that the PII at issue in this case was used by the Center of Excellence, or that Morgan Stanley otherwise benefited or profited from retaining their PII.[9]

Furthermore, unjust enrichment "is not available where it simply duplicates, or replaces, a conventional contract or tort claim." *Corsello* v. *Verizon N.Y., Inc.*, 18 N.Y.3d 777, 790-91 (2012) (citations omitted); *see also Mahoney* v. *Endo Health Sols., Inc.,* No. 15-cv-9841

[9] In the absence of any allegations that Morgan Stanley profited through the Center of Excellence, plaintiffs' reliance on *Rudolph* v. *Hudson's Bay Co*., 18-cv-8472 (PKC), 2019 WL 2023713, at *12 (S.D.N.Y. May 7, 2019), and *Sackin* v. *TransPerfect Global, Inc*., 278 F. Supp. 3d 739, 751 (S.D.N.Y. 2017) is misplaced. (*See* ECF No. 45 at 3.) Both of those cases involved the concrete conferral of a monetary benefit (namely, the purchase of items at a department store and the supply of labor to an employer) whereas Morgan Stanley was not enriched by any allegedly deficient practices.

(DLC), 2016 WL 3951185, at *11 (S.D.N.Y. July 20, 2016). Rather, unjust enrichment "is available only in unusual situations when, though the defendant has not breached a contract nor committed a recognized tort, circumstances create an equitable obligation running from the defendant to the plaintiff." *Corsello,* 18 N.Y.3d at 790; *see also Mahoney*, 2016 WL 3951185, at *11. Here, the unjust enrichment claim fails for the additional reason that it is duplicative of plaintiffs' common law tort claims, rendering it "not available." *Hitachi Data Sys. Credit Corp.* v. *Precision Discovery, Inc.*, 331 F. Supp. 3d 130, 152 (S.D.N.Y. 2018).[10]

D. The State Statutory Claims Should Be Dismissed

Plaintiffs' state statutory claims—based on purported violations of various state data breach notification and protection statutes and unfair and deceptive practices ("UDAP") laws—should likewise be dismissed for failure to plead the elements of those claims with sufficient detail under either the Rule 9(b) or Rule 8(a) standards.

1. Illinois

The elements of a claim under Illinois's UDAP statute—the Illinois Consumer Fraud Act ("ICFA"), 815 Ill. Comp. Stat. 505/1, *et seq.*—are "(1) the defendant undertook a deceptive act or practice; (2) the defendant intended that the plaintiff rely on the deception; (3) the deception occurred in the course of trade and commerce; (4) actual damage to the plaintiff occurred; and (5) the damage complained of was proximately caused by the deception." *Toulon* v. *Cont'l Cas. Co.*, 877 F.3d 725, 739 (7th Cir. 2017) (citation omitted). Where, as here, an

[10] While plaintiffs have argued that they plead unjust enrichment in the alternative to the other claims (*see* ECF No. 45 at 3), the "unjust enrichment claim will not survive a motion to dismiss where the plaintiff[s] fails to explain how it is not merely duplicative of [their] other causes of action." *Tyman* v. *Pfizer, Inc.*, 16-cv-06941 (LTS) (BCM), 2017 WL 6988936, at *20 (S.D.N.Y. Dec. 27, 2017) (citation and punctuation omitted)), *report and recommendation adopted*, 2018 WL 481890, at *1 (S.D.N.Y. Jan. 18, 2018).

ICFA claim is based on fraud, the sufficiency of the complaint is analyzed under the heightened pleading standard set forth in Federal Rule of Civil Procedure 9(b). *Camasta* v. *Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014).[11] Under either the heightened Rule 9(b) or less stringent Rule 8(a) standard, Plaintiffs have not plausibly pleaded any of elements of their ICFA claim.

Under Rule 9(b), plaintiffs' allegations are deficient because they fail to plead what Morgan Stanley's allegedly deceptive practices were, let alone how such practices deceived plaintiffs or how plaintiffs relied on these practices. Rule 9(b) "ordinarily requires describing the 'who, what, when, where, and how' of the fraud, although the exact level of particularity that is required will necessarily differ based on the facts of the case." *Burger* v. *Spark Energy Gas, LLC*, No. 19 C 8231, 2020 WL 7353407, at *3 (N.D. Ill. Dec. 15, 2020) (quoting *AnchorBank, FSB* v. *Hofer*, 649 F.3d 610, 615 (7th Cir. 2011) (citation omitted)). Plaintiffs make no such particularized allegations, and offer no allegations as to how Morgan Stanley deceived its customers in its treatment of their PII.

For similar reasons, plaintiffs have failed to plead any facts—let alone particular facts—that (i) Morgan Stanley intended plaintiffs rely on any alleged deception; or (ii) any alleged deception occurred in the course of trade and commerce. Moreover, plaintiffs offer only threadbare recitations regarding actual damages, and provide no allegations that the damage complained of was proximately caused by the alleged deception to satisfy either the Rule 8(a) or 9(b) pleading standard. *See supra* Part I. *Cf. Thrasher-Lyon* v. *Ill. Farmers Ins. Co.*, 861 F. Supp. 2d 898, 913 (N.D. Ill. 2012) (dismissing ICFA claims, and noting to properly plead

[11] In their December 9, 2020 pre-motion letter to the Court, plaintiffs concede that their ICFA claims are at least partially sourced in deceptive conduct, and thus subject to the heightened pleading standard of Rule 9(b). (*See* ECF No. 45 at 4.)

a ICFA claim "a plaintiff must allege that she suffered specific, actual damages and an allegation of only emotional damages precludes a claim under the ICFA." (citation and internal quotation marks omitted)). For these reasons, plaintiffs' ICFA claim should be dismissed.[12]

2. Pennsylvania

Plaintiffs also bring a claim under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 § 201-2 & 202-3, *et seq.*, for allegedly deceptive acts. (CAC ¶¶ 349–365.) Pleading a claim under the UTPCPL requires a plaintiff plausibly to allege "(1) a deceptive act that is likely to deceive a consumer acting reasonably under similar circumstances; (2) justifiable reliance; and (3) that the plaintiff's justifiable reliance caused ascertainable loss." *Ahmed* v. *Wells Fargo Bank, NA*, 432 F. Supp. 3d 556, 564 (E.D. Pa. 2020). Plaintiffs have failed to plausibly allege any of these elements.

As with their Illinois law claim, plaintiffs have not plausibly alleged a deceptive act by Morgan Stanley. The Complaint makes no plausible allegations about how Morgan Stanley deceived plaintiffs or what allegedly deceptive acts they justifiably relied on. Rather, the gravamen of the complaint is that Morgan Stanley inadvertently misplaced plaintiffs' data. (CAC ¶¶ 1, 6–7.) Similarly, plaintiffs have provided no allegations of reliance (*id.* ¶¶ 349–365), and only the most threadbare recitation of the element of ascertainable loss (*id.* ¶ 361) without any explanation of what that loss is. For these reasons, plaintiffs have failed to state a claim for a violation of the UTPCPL.

---

[12] To the extent plaintiffs allege an ICFA violation based on a predicate violation of 815 Ill. Comp. Stat 530/10(a) (*see* CAC ¶ 334(h)), which requires timely notification of data breaches, this claim also fails. Plaintiffs do not plausibly plead damages, nor that any alleged damages were proximately caused by Morgan Stanley's alleged failure to provide timely notification of the 2016 or 2019 Events.

3. California

California's UDAP statute requires a plaintiff to show an unlawful, unfair, or fraudulent business act or practice. *Irigaray Dairy* v. *Dairy Emp. Union Local No. 17 Christian Labor Ass'n of the U.S. of America Pension Tr.*, 153 F. Supp. 3d 1217, 1256 (E.D. Cal. 2015). The statute "is written in the disjunctive . . . it establishes three [separate] varieties of unfair competition—acts or practices which are unlawful, or unfair, or fraudulent." *Cel–Tech Commc'ns, Inc.* v. *L.A. Cellular Tel. Co.*, 20 Cal.4th 163, 180 (1999) (citation and internal quotation marks omitted). Thus, the claims must be evaluated according to whether they allege unlawful, unfair, or fraudulent business acts. Here, plaintiffs purport to allege unlawful (Count VI) and unfair (Count VII) acts, (CAC ¶¶ 313–325), but have failed to state a claim under either prong.[13]

First, to state a claim under the unlawful prong of the UCL, a plaintiff must show defendant engaged in a practice "forbidden by law, be it civil or criminal, federal, state, or municipal, statutory, regulation, or court-made" and "state with reasonable particularity the facts supporting the elements of the alleged violation." *Carter* v. *Bank of America, N.A.*, No. CV 12-06424 MMM (FFMx), 2012 WL 12887542, at *10 (C.D. Cal. Dec. 12, 2012) (citations and internal quotation marks omitted). Plaintiffs must also plead that they "lost money or property as a result of the unfair competition." *Birdsong* v. *Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009). Here, plaintiffs purport to allege as the predicate unlawful act violations of Cal. Civ. Code § 1798.81.5—which requires entities storing PII to take reasonable methods to safeguard that information—and § 1798.82—which requires businesses that own or license "computerized data

[13] A separate prong of this statute deals with unlawful, unfair, or fraudulent advertising, and is not relevant here.

that includes personal information" to promptly disclose a security breach. But Cal. Civ. Code § 1798.81.5 "do[es] not apply to . . . [a] financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act." Cal. Civ. Code § 1798.81.5(e)(2). Accordingly, while that provision may serve as a predicate for a non-financial institution, it does not apply to financial institutions such as Morgan Stanley. Cal. Civ. Code § 1798.82 similarly only requires a business to notify the residents of a security breach if the "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b). Plaintiffs have made no allegations whatsoever that any PII "was, or [was] reasonably believed to have been, acquired by an unauthorized person." Nor could they, as the Consumer and Attorneys General Notices make clear that Morgan Stanley was "not aware of any access to or misuse of personal information in connection with either of these incidents." (Ex. 1 at 1, Consumer Notice, and Ex. 2 at 3, Attorneys General Notice.) Neither of these statutes can serve as a valid basis for predicate violation for plaintiffs' unlawful acts claim under the UCL.

Even if these statutes were valid predicates for a UCL claim against Morgan Stanley (they are not), plaintiffs have not adequately pleaded that they "lost money or property *as a result* of the unfair competition. *Birdsong*, 590 F.3d at 959 (emphasis added). For the same reasons that plaintiffs have fail to allege injury-in-fact (*see supra* Part I), their conclusory and boilerplate allegations of harm are insufficient for purposes of stating a UCL claim.

Second, an act is "unfair" under the UCL in the consumer context if one of three tests is met: (i) a test based on Section 5 of the Federal Trade Commission Act (the "FTC Test"); (ii) a public policy test requiring that "the UCL claim be tethered to some specific constitutional, statutory, or regulatory provisions" (the "Public Policy Test"); and (iii) a balancing test, in which

an unfair business practice is "one in which the gravity of the harm to the victim outweighs the utility of the defendant's conduct" (the "Balancing Test"). *McVicar* v. *Goodman Global, Inc.*, 1 F. Supp. 3d 1044, 1053–54 (C.D. Cal. 2014) (citation omitted and internal quotation marks omitted)). None can be met here.

The FTC Test, developed in the antitrust context, borrows from Section 5 of the Federal Trade Commission Act and defines "unfair" business practices as those where (1) the consumer injury is substantial, (2) any benefits to consumers or competition does not outweigh the injury, and (3) the consumers could not have reasonably avoided the injury. *Id*. This test has been rejected by the Ninth Circuit in the consumer context, because the test "revolves around anti-competitive conduct, rather than anti-consumer conduct." *Lozano* v. *AT&T Wireless Servs., Inc.*, 504 F.3d 718, 736 (9th Cir. 2007) (citation omitted). Nor does the Public Policy Test apply, because, plaintiffs have made no allegations tying the alleged UCL violation to any constitutional, statutory, or regulatory provision. Thus, to plead a UCL claim, plaintiffs must plausibly allege that some harm that they experienced outweighs the utility of the defendant's conduct under the Balancing Test.

As discussed *supra* Part I, plaintiffs have failed to allege that they have suffered any concrete harm, let alone that this harm outweighed the utility to Morgan Stanley of decommissioning data centers and replacing computer hardware. Because plaintiffs have not alleged, except in the most conclusory fashion, that their alleged harm outweighed any attendant benefits to Morgan Stanley, they have failed to properly plead a violation of the UCL based on unfair conduct.[14]

[14] Even if plaintiffs' claim under the California Unfair Competition Law survives, their relief would be limited to injunctive relief and restitution. *Cel–Tech Commc'ns, Inc.*, 20 Cal.4th at 179.

Separately, Count VIII of the Complaint alleges violations of the California Consumer Privacy Act, Cal. Civ. Code. § 1798.150(a). Plaintiffs' claims under this statute fails for the independent reason that plaintiffs do not allege that any party actually obtained unauthorized access to plaintiffs' PII. *See* Cal. Civ. Code § 1798.150(a). To qualify for protection under that statute, a consumer's PII must have been "subject to an unauthorized access and exfiltration, theft, or disclosure," and that access must also have been "a result of [Morgan Stanley's] violation of [its] duty to implement and maintain reasonable security procedures and practices." *Id.* Here, plaintiffs make no allegation that any PII was accessed, exfiltrated, stolen, or disclosed, and thus plaintiffs' allegations fail to state a claim under the California Consumer Privacy Act. *Cf. Stasi* v. *Inmediata Health Grp. Corp.*, No. 19CV2353 JM (LL), 2020 WL 6799437, at *16 (S.D. Cal. Nov. 19, 2020) (claim for violation of Cal. Civ. Code § 1798.150(a) was properly stated where plaintiffs repeatedly alleged that their information "was viewed by unauthorized persons").[15]

4. New York

New York's UDAP provision, New York Gen. Bus. Law § 349, requires the plaintiff plausibly allege that the defendant "engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." *City of New York* v. *Smokes-Spirits.Com, Inc.*, 12 N.Y.3d 616, 621 (2009). Plaintiffs have failed to plausibly allege a misleading act that caused injury.

Specifically, plaintiffs have failed to plead any injury as a result of deception by Morgan Stanley. They have not alleged that their damages, if any, (i) occurred as a result of any

[15] The California Consumer Privacy Act also does not apply because it only came into effect January 1, 2020, after the 2016 and 2019 Events.

materially misleading representations Morgan Stanley made about its data security practices; or (ii) were caused by the 2016 or 2019 Events. *See Jensen* v. *Cablevision Sys. Corp.*, 372 F. Supp. 3d 95, 127–28 (E.D.N.Y. 2019) ("The *potential* for the release of private information, without any evidence of the *actual* release of private information, by itself, does not constitute an injury sufficient to state a claim" in the GBL § 349 context); *Shostack* v. *Diller*, No. 15-CV-2255 GBD JLC, 2015 WL 5535808, at *8 (S.D.N.Y. Sept. 16, 2015) ("Although the actions of the unknown third party who misappropriated [plaintiff's] identity were undoubtedly fraudulent, there was nothing deceptive about Lending Tree running [plaintiff's] credit report"), *report and recommendation adopted,* No. 15CIV2255GBDJLC, 2016 WL 958687 (S.D.N.Y. Mar. 8, 2016). Thus, their claim under New York's UDAP statute also fails.[16]

CONCLUSION

For the foregoing reasons, Defendant Morgan Stanley respectfully requests that Plaintiffs' Complaint be dismissed with prejudice.

[16] Plaintiffs agreed to dismiss their claim under New York Gen. Bus. Law § 899-aa. *See* Plaintiffs' Pre-Motion Letter to the Court, ECF No. 45 at 4.

Dated: Washington, D.C.
January 14, 2021

PAUL, WEISS, RIFKIND, WHARTON &
GARRISON LLP

By: */s/ Jane B. O'Brien*

Brad S. Karp
Susanna M. Buergel
Anika Rappleye
1285 Avenue of the Americas
New York, New York 10019
Telephone: (212) 373-3000
Facsimile: (212) 757-3990
bkarp@paulweiss.com
sbuergel@paulweiss.com
arappleye@paulweiss.com

Jane B. O'Brien
Crystal Johnson Geise
2001 K Street NW
Washington, DC 20006
Telephone: (202) 223-7300
Facsimile: (202) 223-7420
jobrien@paulweiss.com
cgeise@paulweiss.com

Attorneys for Defendant
Morgan Stanley Smith Barney LLC